UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,310	12/12/2003	Leonard D. Rarick	SUNMP349	1691

32291 7590 04/15/2008

MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
04/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/734,310	RARICK ET AL.	
	Examiner	Art Unit	
	HARRIS C. WANG	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-10,12,14 and 18-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-4, 7-10, 12, 14, 18-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/04/2008 has been entered.

Claim Objections

Claims 1-4, 7-10, 12, 14, 18-20 objected to because of the following informalities: The Applicant throughout the claims has used the limitation "crypto." While it is understood what the Applicant intends, using the full version "cryptographic" is more appropriate for the use in formal claims. Therefore the Examiner suggests replacing all instances of the word "crypto" with "cryptographic." Appropriate correction is required.

Claims 2-3 are objected because of the following informalities. The Applicant has used the limitation "muxes." While it is understood the Applicant intends, using the full version "multiplexers" is more appropriate for the use in formal claims. Therefore the Examiner suggests replacing "muxes" with "multiplexers." Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-4, 7-10, 12, 14,18-20 rejected under 35 U.S.C. 103(a) as being unpatentable over Zakiya in view of Qi..

Regarding Claim 1, 7, 10, 19

Zakiya teaches a cryptographic algorithm unit comprising:

A first cryptographic hash execution module;

A second cryptographic hash execution module, wherein the first cryptographic execution module and the second cryptographic execution module share a plurality of components to form a combination cryptographic execution module unit, wherein the combination cryptographic algorithm unit being capable of performing an MD5 hash algorithm and a SHA1 hash algorithm *(Figure 10 is a block diagram of a multi-hash structure to implement both MD5 and SHA1, the Examiner interprets the module for performing MD5 as the first cryptographic hash execution module, and the module for performing SHA1 as the second cryptographic hash execution module. Figure 10 shows the structure sharing a plurality of components. Paragraph [0045] describes the combination structure in detail),* the combination cryptographic algorithm unit including:

A first summing circuit, the first summing circuit being a four input summing circuit with a single first summing circuit output. (Figure 9 shows a four input summing circuit with a single first summing circuit output. The Examiner interprets the first input as *(Figure 9, 901, "A").* The Examiner interprets the second input as *(Figure 9, 906, "hi").* The Examiner interprets the third and fourth input as *(Figure 9, 907, "WKi")* which is the combination of the W and Ki inputs *("Wki 907 (Wi + Ki) sum for the round" paragraph [0044])* For clarification, the input A would correspond with the Applicant's "A" in figure 7, "hi" corresponds to the Applicants "functions of B,C,D" and "Wki" correspond to the Applicant's X and Y)

A second summing circuit, the second summing circuit being

Wherein a first input to the second summing circuit is coupled to the first summing circuit output, wherein the first summing circuit output is coupled to the first input to the second summing circuit through a rotate circuit during an MD5 hash

algorithm; *(Figure 9, **943**, shows the second summing circuit. Where the first summing circuit output is coupled to the first input to the second summing circuit through a rotate circuit during an MD5 hash, **960**)*

Wherein a SHA1 chaining variable is coupled to the second input to the second summing circuit during a SHA1 hash algorithm and wherein an MD5 chaining variable is coupled to the second input to the second summing circuit during an Md5 hash algorithm. *(Figure 9 shows a SHA1 chaining variable and a MD5 chaining variable connected to the second input of the second summing circuit, **905**, where B and E are the chaining variables entered into the second summing circuit **943**)*

Zakiya does not explicitly teach wherein the first summing circuit includes a four to two compressor and a first carry look-ahead adder wherein the four to two compressor is a two output device and the two outputs are coupled to each of two inputs to the first carry look-ahead adder, the first carry look-ahead adder having the first summing circuit output. Zakiya does not explicitly teach wherein the second summing circuit is a second two input carry look ahead adder.

Qi teaches using a 4 to 2 compressor input into a Carry Look-ahead Adder *(Figure 9B, add4to1)*. Although the figure says it is a "4 to 1 adder," Qi takes 4 inputs and compresses it into 2, **C** and **D**, before inputting to a CLA which then outputs one output. This is similar to the Applicant's Figure **7**, where 4 inputs are compressed into 2, before inputting into a CLA which then outputs one output. Qi teaches that CLAs are generally composed of full adders (Paragraph **[0048]**).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to substitute the first and second adders of Zakiya with the 4 to 2 compressor and CLA adder as described by Qi.

The references are combinable because both Zakiya and Qi are directed to SHA and MD5 hash functions (as seen on Figure 1 of Qi and the already cited portions of Zakiya). The motivation for combining can be found in Paragraph [0058] of Qi *("A CLA is designed to reduce the carry propagation delay").*

Regarding Claims 2-4, 20

Zakiya and Qi teach the cryptographic algorithm unit of claims 1 and 19, wherein the combination crypto algorithm unit includes a plurality of multiplexers wherein the multiplexers provide cryptographic hash algorithm selection control. *(Figure 8, shows a multiplexer, figure 9, **935**, shows another multiplexer.)* Wherein the cryptographic hash algorithm selection control allows the selection of a first subset of the plurality of components, wherein the selected first subset of the plurality of components can execute a first cryptographic algorithm. *("A multiplexer 935 Selects B or E to be added at 943. the elements 930, 950, and 960 represent the logic to perform the necessary rotate operations for each hash" Paragraph [0044])*

Regarding Claims 7-8, 14, 18

Zakiya and Qi teach the cryptographic algorithm unit of claim 1. However Zakiya does not explicitly teach wherein the combination cryptographic unit and a microprocessor are on a single integrated circuit die.

The Examiner takes Official Notice that it is common to put microprocessors and circuits on a single integrated circuit die, such as a "System-on-a-chip".

It would have been obvious to one of ordinary skill in the art at the time of the invention to put a circuit taught by Zakiya and Qi and a microprocessor on a single integrated circuit die.

The motivation is to save space.

Regarding Claim 12,

Zakiya and Qi teach the cryptographic algorithm unit of claim 1. Zakiya teaches that the cryptographic algorithm unit includes a plurality of compressors.

The Examiner interprets a compressor as any circuit unit that receives multiple inputs and compresses them into fewer outputs. Therefore the Examiner interprets each adder, which takes in two inputs and outputting one output as a separate compressor. Therefore Figure 9 shows a plurality of compressors.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HARRIS C. WANG whose telephone number is (571)270-1462. The examiner can normally be reached on M-F 9-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KRISTINE KINCAID can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139